ПРАВОВЫЕ ОСНОВЫ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В УКРАИНЕ

Онищенко Ю.Н., Рудик А.С.

Харьковский национальный университет внутренних дел
Харьковский национальный университет радиоэлектроники

Защита конфиденциальной информации, циркулирующей (передаваемой, принимаемой), обрабатываемой и/или хранящейся в специальных информационно-телекоммуникационных и других системах, обеспечивается применением средств криптографической защиты информации (КЗИ), а также выполнением соответствующих организационно-технических и режимных мероприятий.

Основными нормативно-правовыми актами, регулирующими использование криптографии в Украине, являются законы Украины: «Про информацию», «Про научно-техническую информацию», «Про защиту информации в информационно-телекоммуникационных системах», «Про государственную тайну», «Про Национальную систему конфиденциальной связи», «Про электронную цифровую подпись» [1,2,3].

Криптографическая защита информации - вид защиты информации, реализующийся путем преобразования информации с использованием специальных (ключевых) данных с целью сокрытия (или восстановления) содержания информации, подтверждения ее подлинности, целостности, авторства и т.д. [3].

Средства КЗИ должны разрабатываться с учетом возможных угроз со стороны среды, в которой предполагается их применение. Разработчик должен предусмотреть организационно-технические мероприятия по защите от несанкционированного доступа, контролю целостности программного обеспечения средства криптографической защиты, обеспечению надежного механизма тестирования средства КЗИ на правильность функционирования, а также обязательное блокирование работы средства КЗИ в случае выявления нарушений.

В средствах КЗИ должны использоваться криптоалгоритмы и криптопротоколы, которые являются государственными стандартами Украины. Для разработки средств КЗИ используется только лицензионное программное обеспечение. В зависимости от способа реализации различают следующие типы средств КЗИ:

– аппаратные средства, алгоритмы функционирования которых реализуются в оптических, механических микроэлектронных или других специализированных устройствах и не могут быть изменены во время эксплуатации;

– аппаратно-программные средства, алгоритм функционирования которых реализуется с помощью программного обеспечения, которое устанавливается при производстве средства КЗИ в специальном запоминающем

устройстве, выполняется в нем и может быть изменено только при производстве;

– программные средства, алгоритм функционирования которых реализуется программным обеспечением, функционирующий под управлением операционных систем электронно-вычислительной техники; отдельные функции программного средства криптографической защиты могут выполняться аппаратными или аппаратно-программными устройствами, функционирующими под управлением программного обеспечения средства КЗИ [4].

Обычно пользователь аппаратных средств КЗИ не имеет доступа к содержанию запоминающих элементов, хранящих микропрограммы управления устройством, алгоритм функционирования устройства меняется только их разработчиком или изготовителем.

Средства КЗИ без введенных ключевых данных имеют гриф ограничения доступа, который соответствует грифу ограничения доступа описания криптосхемы. Гриф ограничения доступа средств КЗИ с введенными ключевыми данными определяется грифом ограничения доступа ключевых документов, но не ниже грифа ограничения доступа описания криптосхемы. Гриф ограничения доступа ключевых документов, используемых для КЗИ, должен отвечать грифу ограничения доступа защищаемой информации.

В соответствии с Законом Украины «Про лицензирование видов хозяйственной деятельности», с учетом особенностей, указанных в Законе Украины «Про телекоммуникации», субъекты, осуществляющие разработку, производство и эксплуатацию средств КЗИ, определяют режим доступа к информации об этих средствах, устанавливают и поддерживают соответствующий режим безопасности с учетом требований заказчика и в соответствии с нормативно-правовыми актами в сфере КЗИ.

В настоящее время методы и средства криптографии используют для обеспечения информационной безопасности не только государства, но и частных лиц и организаций, реализуя различные механизмы защиты конфиденциальности, целостности, доступности и полноты информации.

1. Про Национальную систему конфиденциальной связи : Закон Украины от 10.01.2002 № 2919-III : [редакция от 19 апреля 2014 г.] // ВВР Украины. – 2002. – № 15. – Ст. 103. Режим доступа : http://zakon.rada.gov.ua/laws/show/2919-14.
2. Про утверждение Положения про государственный контроль за состоянием технической защиты информации : приказ Администрации Государственной службы специальной связи и защиты информации Украины от 16.05.2007 № 87 : [редакция от 10 марта 2015 г.]. – Режим доступа: http://zakon.rada.gov.ua/laws/show/z0785-07.
3. Про защиту информации в информационно-телекомуникационных системах : закон Украины от 05.07.1994 № 80/94-ВР : [редакция от 19 апреля 2014 г.] // ВВР Украины. – 1994. – № 31. – Ст. 286. – Режим доступа: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
4. Богуш В.М. Информационная безопасность государства : уч. пособ. / В.М. Богуш, А.К. Юдин. – К.: МК-Прес, 2005. – 432 с.